Interpolation und Kettenbruchentwicklung. Die Komplexität einiger Berechnungsaufgaben.

INAUGURAL-DISSERTATION

zur Erlangung der philosophischen Doktorwürde
vorgelegt der
Philosophischen Fakultät II der Universität Zürich

von

PETER SCHUSTER
aus Deutschland

Begutachtet von Herrn Prof. Dr. V. Strassen

Zürich 1980

INTERPOLATION UND KETTENBRUCHENTWICKLUNG. DIE KOMPLEXITÄT EINIGER BERECHNUNGSAUFGABEN

Inaugural - Dissertation

zur Erlangung der philosophischen Doktorwürde

vorgelegt der

Philosophischen Fakultät II

der Universität Zürich

von

Peter Schuster

aus Deutschland

Begutachtet von Herrn Prof. Dr. V. Strassen

Zürich 1980


UNIV.
LEIDEN
BIBL.

INHALT

	Vorbemerkung	2
§ 1	Symmetrische Probleme	4
§ 2	Auswerten der s-ten Ableitung eines Interpolationspolynoms an den Stützstellen	7
§ 3	Bestimmung der Gradzahlen in der Euklidischen Entwicklung eines Polynompaares	10
§ 4	Das Rechnen mit Kettenbrüchen	21
	Literatur	27

Digitized by the Internet Archive
in 2026

https://archive.org/details/IA41507208_0031

VORBEMERKUNG

In dieser Arbeit werden gewisse Berechnungsaufgaben behandelt, die beim Rechnen mit Polynomen und rationalen Funktionen in einer Variablen über einem unendlichen Körper K auftreten.

Berechnungen werden an endlich vielen Ausgangsdaten ausgeführt (z.B. an den Koeffizienten eines Polynoms). Im Falle von Berechnungen ohne Verzweigungen werden diese durch Unbestimmte repräsentiert, Berechnungen verlaufen also in einem rationalen Funktionenkörper mit mehreren Unbestimmten über K. Wir betrachten Additionen, Subtraktionen und Skalarmultiplikationen als kostenlos und zählen die nichtskalaren Multiplikationen und Divisionen. Dies legt für jede endliche Menge E von rationalen Funktionen in den Unbestimmten die multiplikative Komplexität L(E) fest, nämlich den kleinstmöglichen Aufwand zur Berechnung von E.

Lässt man auch Berechnungen zu, die Vergleiche ausführen und daraufhin verzweigen, wird man als grobes Mass für die Länge eines Algorithmus dessen Aufwand im langwierigsten Fall nehmen, wieder bei Zählung allein der nichtskalaren Multiplikationen und Divisionen, und die Komplexität einer Berechnungsaufgabe ist dann die Länge eines kürzesten Algorithmus, der die Aufgabe löst. (Ein feineres Komplexitätsmass aus Strassen [13] behandeln wir in § 3.)

In diesem Sinne einer " Untersuchung des schwierigsten Falles " zeigen wir: Die Darstellung rationaler Funktionen als Kettenbrüche verringert der Grössenordnung nach nicht die Komplexität der Grundrechenarten Addition, Multiplikation, Division sowie des Auswertens an vielen Stellen - immer im Vergleich zur Darstellung der

rationalen Funktionen durch die Koeffizienten von Zählerpolynom und normiertem Nennerpolynom in gekürzter Form. Ist das Kürzen der Grössenordnung nach leichter als die Berechnung der ganzen Kettenbruchentwicklung, so ist die Kettenbruchdarstellung sogar ungünstiger für die Ausführung von Addition und Multiplikation (§4). Die multiplikative Komplexität der Kettenbruchentwicklung ist seit den Arbeiten von Schönhage [8] und Strassen [12] der Grössenordnung nach völlig bekannt. Dass bereits die Bestimmung der "Form" des Kettenbruchs (d.h. der Gradzahlen der darin auftretenden Polynome) "im schwierigsten Fall" etwa gleich schwierig ist, zeigen wir in § 3. (Hier setzen wir K als algebraisch abgeschlossen voraus.)

In § 2 verallgemeinern wir ein Resultat von Strassen [14] : Wir schätzen ab, wie schwierig es ist, eine höhere Ableitung eines Interpolationspolynoms an dessen Stützstellen (wo das Polynom vorgegeben ist) auszuwerten, und zwar auch über Körpern positiver Charakteristik.

Schliesslich nennen wir in § 1 die Konventionen, die wir hier stets benutzen. Fundamental für alle unteren Komplexitätsschranken in dieser Arbeit ist die Gradmethode von Strassen. Daher drücken wir vieles in der Sprache der algebraischen Geometrie aus. Auch ein ganz allgemeines Prinzip, das sich aus der Gradmethode ergibt und eine erste Anwendung aus [10] verallgemeinert, ist in diesem ersten Paragraphen verzeichnet.

Mein herzlicher Dank gilt Prof. V. Strassen für die beständige Unterstützung bei dieser Arbeit. Auch die Anregung zu diesem Thema verdanke ich ihm.

§ 1. SYMMETRISCHE PROBLEME

Wir fassen $K(x_1,\dots,x_n) = K(\underline{x})$ als K-Algebra über den Konstanten und den Unbestimmten auf, d.h. über $K \cup \{x_1,\dots,x_n\}$, und bezeichnen mit $L(E)$ die multiplikative Komplexität einer endlichen Menge $E \subset K(\underline{x})$. Zur Abschätzung von L nach unten werden wir stets und ohne Beschränkung der Allgemeinheit K als algebraisch abgeschlossen voraussetzen.

Die zugehörigen Räume K^m denken wir uns mit der Zariski-Topologie versehen. Die darin lokal abgeschlossenen Teilmengen sind die in dieser Arbeit auftretenden Varietäten.

Der Grad $\deg I$ einer irreduziblen Varietät I in K^m ist die typische Schnittpunktzahl von I mit einem affinen linearen Teilraum komplementärer Dimension. Der Grad einer beliebigen Varietät V in K^m ist dann durch die Gradzahlen ihrer irreduziblen Komponenten $I_1,\dots,I_r$ definiert:

$$\deg V = \sum_{\varsigma=1}^{r} \deg I_\varsigma .$$

Verschiedentlich werden wir die Ungleichungen von Bezout benutzen: <u>Es seien</u> $I_1,\dots,I_r$ <u>die irreduziblen Komponenten des Durchschnitts der Varietäten</u> V <u>und</u> W <u>in</u> K^m. <u>Dann gilt für die Gradzahlen in</u> K^m:

$$\deg V \cap W \leq \deg V \cdot \deg W.$$

(Hier ist die Eigentlichkeit der Durchschnitte nicht verlangt.) Für einen elementaren Beweis siehe Heintz [5].

Speziell gilt also:

(1) W affin linear, $V \cap W$ endlich $\Rightarrow$ $\# V \cap W \leq \deg V$.

Grundlegend für alles weitere ist nun der

SATZ (Strassen [10]). Es seien $f_1,\dots,f_r \in K(\underline{x})$ und φ die durch $(f_1,\dots,f_r)$ vermittelte rationale Abbildung, d.h.

$$\text{graph}\ \varphi = \left\{(u_1,\dots,u_n,\ f_1(\underline{u}),\dots,f_r(\underline{u})): \forall \varsigma \leq r\ f_\varsigma(\underline{u}) \text{ definiert}\right\} \subset K^{n+r}.$$

Dann ist

$$\lg \deg(\text{graph}\ \varphi) \leq L(f_1,\dots,f_r).$$

In diesem Satz ist wieder K als algebraisch abgeschlossen vorausgesetzt. Mit lg bezeichnen wir stets den Binär-Logarithmus. Zu irreduziblen $V \subset K^m$ werden wir manche Aussage "für fast alle $\underline{v}$ aus V" machen. Wir meinen damit, die Aussage gelte mindestens auf einem nichtleeren offenen Teil von V.

Als erstes beweisen wir folgende Verallgemeinerung der unteren Schranke in Satz 3.1. von Strassen [10]:

SATZ 1. Es seien $f_1,\dots,f_r \in K(\underline{x})$, $\text{trdeg}\{f_1,\dots,f_r\} = n$, und G die (endliche) Gruppe der K-Automorphismen, die alle f_ς festlassen. Dann ist

$$\lg \# G \leq L(f_1,\dots,f_r).$$

BEWEIS: O.B.d.A. ist $r = n$. Es sei φ die durch $(f_1,\dots,f_n)$ vermittelte rationale Abbildung von K^n nach K^n. Wegen (1) genügt es, einen Punkt $\underline{v} \in K^n$ zu finden, für den $\varphi^{-1}(\underline{v})$ endlich und $\#\varphi^{-1}(\underline{v}) \geq \# G$ ist. (Man schneidet graph φ mit $K^n \times \{\underline{v}\}$ in K^{2n}.)

Die K-Automorphismengruppe von $K(\underline{x})$ ist isomorph zur Gruppe der birationalen Automorphismen von K^n. Jedes $g \in G$ können wir damit als birationalen Automorphismus von K^n auffassen: $g(\underline{u}) := (g(x_1),\dots,g(x_n))(\underline{u})$, vorausgesetzt, $\underline{u} \in K^n$ liegt im Definitionsbereich von $(g(x_1),\dots,g(x_n))$. Da die φ definierenden rationalen Funktionen G-invariant sind, gilt

$(\underline{u} \in \mathrm{Def}\, g \;\&\; \underline{u} \in \mathrm{Def}\,\varphi) \Rightarrow g(\underline{u}) \in \varphi^{-1}\varphi(\underline{u})$.

Für fast alle $\underline{u} \in K^n$ gilt:

(i) $\underline{u} \in \mathrm{Def}\,\varphi$,

(ii) $\varphi^{-1}\varphi(\underline{u})$ endlich,

(iii) $\forall\, g \in G \quad \underline{u} \in \mathrm{Def}\, g$,

(iv) $\# G\underline{u} = \# G$.

Für ein solches $\underline{u}$ ist dann $\#\varphi^{-1}\varphi(\underline{u})$ endlich und $\#\varphi^{-1}\varphi(\underline{u}) \geq \# G\underline{u} = \# G$.

§ 1. AUSWERTEN DER s-TEN ABLEITUNG EINES INTERPOLATIONSPOLYNOMS AN DEN STÜTZSTELLEN

Hier behandeln wir die Aufgabe, die s-te Ableitung eines Interpolationspolynoms P – gegeben durch die Stützstellen $x_o,\dots,x_n$ und die Werte $y_o,\dots,y_n$ – an dessen Stützstellen $x_o,\dots,x_n$ auszuwerten. Zu Unbestimmten $x_o,\dots,x_n$, $y_o,\dots,y_n$ über dem Körper K sei $P \in K(\underline{x},\underline{y})[T]$ das Polynom vom Grade n mit

$$\forall \nu \qquad P(x_\nu) = y_\nu \; .$$

Für festes $s > o$ (mit $s < \mathrm{char}\, K$ bei positiver Charakteristik) zeigen wir von der s-ten Ableitung $P^{(s)}$ von P nach T :

$$L(P^{(s)}(x_o),\dots,P^{(s)}(x_n)) \asymp n \cdot \lg n.$$

(L ist die multiplikative Komplexität in $K(\underline{x},\underline{y})$ über $K \cup \{x_o,\dots,x_n, y_o,\dots,y_n\}$.) Dies verallgemeinert ein Resultat von Strassen [14].

Mit den schnellen Algorithmen zur Berechnung der Koeffizienten von P, dem trivialen Differentiationsalgorithmus für Polynome in Koeffizientendarstellung und den schnellen Algorithmen zur Auswertung von $P^{(s)}$ an den Stellen $x_o,\dots,x_n$ (Horowitz [6], Fiduccia [4], Borodin-Moenck [2], Sieveking [9], Strassen [11]) erhalten wir

$$L(P^{(s)}(x_o),\dots,P^{(s)}(x_n)) = O(n \cdot \lg n).$$

SATZ 2. _Sei_ $o < s \leq n$. _Dann ist_

$$n \cdot \lg \frac{n}{s+1} \leq L(P^{(s)}(x_o),\dots,P^{(s)}(x_n)),$$

falls $\mathrm{char}\, K = o$.

Mit $m := \deg P^{(s)}$ gilt bei positiver Charakteristik

$$\frac{n}{2} \cdot \lg \frac{m+s}{s+1} \leq L(P^{(s)}(x_o),\ldots,P^{(s)}(x_n)).$$

BEWEIS. Die hier betrachtete rationale Abbildung φ von K^{2n+2} nach K^{n+1} bildet $(\underline{u},\underline{v}) \in K^{2n+2}$ mit paarweise verschiedenen $u_o,\ldots,u_n$ so ab: Ist p das Interpolationspolynom der Werte v_i an den Stützstellen u_i, so ist $\varphi(\underline{u},\underline{v}) = (p^{(s)}(u_o),\ldots,p^{(s)}(u_n))$. Es genügt nun

$$\deg \operatorname{graph} \varphi \geq \left(\frac{m+s}{s+1}\right)^{n-l}$$

mit $m := \deg P^{(s)}$ und

$$l := \begin{cases} o \text{ falls } \operatorname{char} K = o \\ \lfloor\frac{m}{\chi}\rfloor \text{ falls } \chi := \operatorname{char} K \neq o \end{cases}$$

zu zeigen. Hierzu geben wir eine Varietät $V \subset K^{3n+3}$ an, die graph φ in einer endlichen Menge schneidet. Die Ungleichung von Bezout liefert dann

$$\deg \operatorname{graph} \varphi \geq \frac{\#(V \cap \operatorname{graph} \varphi)}{\deg V}.$$

V wählen wir so, dass in $V \cap \operatorname{graph} \varphi$ nur solche Punkte liegen, die zu dem festen Interpolationspolynom $p = T^{m+s}$ gehören. Für dieses gilt die Gleichung

$$T^s \cdot p^{(s)} = (m+s)_s \cdot p .$$

(Es ist $(\nu)_s := \nu \cdot (\nu-1) \cdot \ldots \cdot (\nu-s+1)$.) Anschaulich gesprochen wird in V die Gültigkeit dieser Differentialgleichung an sämtlichen Stützstellen verlangt, $l+1$ Stützstellen werden als $a_o,\ldots,a_l$ fixiert, ebenso die Werte an diesen Stellen als

$b_o = a_o^{m+s}, \ldots, b_l = a_l^{m+s}$ ("Randbedingung"). Schliesslich legen wir auch noch die Werte in den nicht fixierten Stützstellen als $b_{l+1}, \ldots, b_n$ fest. Die a_ν, b_ν seien so in K gewählt, dass $b_o, \ldots, b_n$ untereinander und von 0 verschieden sind und dass – wie gesagt –, $\forall \nu \leq l \quad b_\nu = a_\nu^{m+s}$ gilt:

$$V := \{(u_o, \ldots, u_n, v_o, \ldots, v_n, w_o, \ldots, w_n) : \forall \nu \;\; v_\nu = b_\nu ,\; u_\nu^s \cdot w_\nu = (m+s)_s \cdot v_\nu ,\; \forall \nu \leq l \quad u_\nu = a_\nu \}$$

Wir zeigen nun, dass V und graph φ sich in der Menge

$S := \{ (\underline{u}, \underline{v}, \underline{w}) \in \text{graph}\, \varphi : \forall \nu \quad u_\nu^{m+s} = v_\nu = b_\nu ,\; \forall \nu \leq l \quad u_\nu = a_\nu \}$ schneiden:

$S \subset V \cap \text{graph}\, \varphi$ ist offensichtlich, und aus $(\underline{u}, \underline{v}, \underline{w}) \in V \cap \text{graph}\, \varphi$ folgt für das Interpolationspolynom $p = \sum_{\nu=o}^{n} p_\nu \cdot T^\nu$ der Werteliste $\underline{v}$ an den Stellen $\underline{u}$:

$$\sum_{\nu=s}^{n} (\nu)_s \cdot p_\nu \cdot T^\nu = (m+s)_s \cdot \sum_{\nu=o}^{n} p_\nu \cdot T^\nu .$$

$\chi :=$ char K teilt $(m+s)_s$ nicht, mithin ist $p_\nu = o$, wenn $(\nu)_s \not\equiv (m+s)_s \bmod \chi$. Es ist also $p = \sum_{\lambda=o}^{l} p_{\lambda \cdot \chi + \mu} \cdot T^{\lambda \cdot \chi + \mu}$, wo μ das kleinste $\nu \in \mathbb{N}$ mit $(\nu)_s \equiv (m+s)_s \bmod \chi$ ist.

Die Definition von V legt nun

$$\forall \nu \leq l \qquad p(a_\nu) = \sum_{\lambda=o}^{l} p_{\lambda \cdot \chi + \mu} \cdot a_\nu^{\lambda \cdot \chi + \mu} = a_\nu^{m+s}$$

fest. Kürzen wir mit $a_\nu^\mu \in K^\times$, so finden wir

$$\forall \nu \leq l \qquad \sum_{\lambda=o}^{l} p_{\lambda \cdot \chi + \mu} (a_\nu^\chi)^\lambda = (a_\nu^\chi)^l .$$

Da die a_ν^χ paarweise verschieden sind, folgt $p = T^{\chi l + \mu} = T^{m+s}$ und damit $(\underline{u}, \underline{v}, \underline{w}) \in S$.

Schliesslich ist $\# S = (m+s)^{n-l}$ weil für jedes ν $T^{m+s} - b_\nu$ nur einfache Nullstellen hat, und es ist $\deg V \leq (s+1)^{n-l}$.

§ 3 BESTIMMUNG DER GRADZAHLEN IN DER EUKLIDISCHEN ENTWICKLUNG EINES POLYNOMPAARES

In diesem Paragraphen sei K ein algebraisch abgeschlossener Körper.

Zu einem Paar von Polynomen $A_o, A_1 \in K[T] \setminus \{o\}$ mit $n_o := \deg A_o \geq n_1 := \deg A_1$ liefert der Euklidische Algorithmus

$$
(2) \qquad
\begin{aligned}
A_o &= Q_o \cdot A_1 + A_2 \\
&\vdots \\
A_\lambda &= Q_\lambda \cdot A_{\lambda+1} + A_{\lambda+2} \quad \text{mit} \quad \deg A_{\lambda+2} < \deg A_{\lambda+1} \\
&\vdots \\
A_{l-1} &= Q_{l-1} \cdot A_l
\end{aligned}
$$

die sogenannte Euklidische Entwicklung $(Q_o, Q_1, \ldots, Q_{l-1}, A_l)$ von (A_o, A_1). Charakteristisch für die Euklidische Entwicklung $(Q_o, \ldots, A_l)$ von (A_o, A_1) ist

$$
(3) \quad \begin{pmatrix} A_o \\ A_1 \end{pmatrix} = \begin{pmatrix} Q_o & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} Q_1 & 1 \\ 1 & 0 \end{pmatrix} \cdot \ldots \cdot \begin{pmatrix} Q_{l-1} & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} A_l \\ 0 \end{pmatrix} , \quad \forall \lambda \geq 1 \ \deg Q_\lambda \geq 1
$$

oder auch

$$
(4) \quad A_o = [Q_o, \ldots, Q_{l-1}] \cdot A_l, \quad A_1 = [Q_1, \ldots, Q_{l-1}] \cdot A_l, \forall \lambda \geq 1 \ \deg Q_\lambda \geq 1,
$$

worin das Eulersche Symbol $[Q_o, \ldots, Q_{l-1}]$ die Summe aus $Q_o \cdot \ldots \cdot Q_{l-1}$ und allen Teilprodukten ist, die durch Streichen aller möglichen Paare benachbarter Faktoren entstehen.

Schönhage gibt in [8] einen Algorithmus zur Kettenbruchentwicklung von Zahlen an, der sich leicht auf Polynome übertragen lässt und dann aus den Koeffizienten von A_o und A_1 die

der Euklidischen Entwicklung ($m_\lambda := \deg Q_\lambda$, $m_l := \deg A_l$) mit höchstens

$$45 \cdot \sum_{\lambda=0}^{l} (m_l \cdot \lg \frac{n_0}{m_\lambda}) + 235 \cdot n_0$$

nichtskalaren Multiplikationen berechnet (siehe auch Moenck [7] und Strassen [13]). Dies ist bis auf einen konstanten Faktor optimal (Strassen [12] , [13]).

Wir referieren hier das für dieses Resultat aus [13] benutzte Werkzeug: Betrachtet werden Algorithmen, die neben den Inputs $\underline{x} \in K^n$ (in diesem Falle $n = n_0+n_1+2$) und den Konstanten $0,1 \in K$ K-Linearkombinationen, Multiplikationen, Divisionen und Verzweigungen gemäss "$v = o$?" für unterwegs berechnete $v \in K$ benutzen.

So entsteht ein Berechnungsbaum, der insgesamt eine Fuktion $f : K^n \longrightarrow \bigcup_{m \in \mathbb{N}} K^m$ sowie eine endliche Partition π von K^n definiert. Die Partition wird durch die Verzweigungen erzeugt, jedes $D \in \pi$ ist also lokal abgeschlossen in K^n.
Im D definierenden Blatt des Berechnungsgraphen wird die Funktion $f\restriction_D$ berechnet, sie ist ein Morphismus von D nach $K^{r(D)}$.

Der Algorithmus berechnet (π, f) in der Zeit $t:K^n \longrightarrow [o,\infty[$ ("strikt" im Sinne von [13]), wenn er für jedes $D \in \pi$ und jedes $\underline{x} \in D$ nicht mehr als $t(\underline{x})$ nichtskalare Multiplikationen und Divisionen auf dem Pfad in das zu D gehörende Blatt ausführt. Wir sagen, irgendeine Funktion $f:K^n \longrightarrow \bigcup_{m \in \mathbb{N}} K^m$ ist in der Zeit t berechenbar, wenn es ein π gibt, so dass sich (π, f) in der Zeit t berechnen lässt.

Es gilt nun der

SATZ (Strassen [13]). Ist (π, f) in der Zeit t berechenbar und ist $D \in \pi$, so ist $\forall\, \underline{x} \in D \quad \log \deg(\text{graph } f \restriction_D) \leq t(\underline{x})$.

Wir werden diesen Satz benutzen, um die Komplexität verschiedener, mit der Euklidischen Entwicklung zusammenhängender Funktionen nach unten abzuschätzen.

Hierfür benötigen wir einige (zum grössten Teil in [3] von Collins und in Ansätzen schon bei Bôcher [1] verzeichnete) Aussagen über Untermatrizen der zu

$$A_o = \sum_{\nu=o}^{n_o} a_{o,\nu} \cdot T^{\nu} \quad \text{und} \quad A_1 = \sum_{\nu=o}^{n_1} a_{1,\nu} \cdot T^{\nu}, \quad a_{o,n_o} \cdot a_{1,n_1} \neq o,$$

gehörenden Resultantenmatrix

$$(r_{\mu,\nu})_{\substack{\mu=1,\dots,n_o+n_1 \\ \nu=1,\dots,n_o+n_1}} = \begin{pmatrix} a_{o,n_o} & \cdots & a_{o,1} & a_{o,o} & & 0 \\ & \ddots & & & \ddots & \\ & & a_{o,n_o} & \cdots & a_{o,1} & a_{o,o} \\ 0 & & & a_{1,n_1} & \cdots & a_{1,o} \\ & & \cdot^{\cdot^{\cdot}} & & \cdot^{\cdot^{\cdot}} & \\ & & & & & 0 \\ a_{1,n_1} & \cdots & a_{1,o} & & & \end{pmatrix}$$

Im folgenden setzen wir stets $n_o \geqslant n_1$ voraus. Für jedes Indexpaar (i,j) mit $o \leq i \leq j \leq n_1$ nennen wir

$$S_{j,i}(A_o,A_1) := \det\, (r_{\mu,\nu})_{\substack{\mu = j+1,\dots,n_o+n_1-j \\ \nu = j+1,\dots,n_o+n_1-j-1,\; n_o+n_1-i}}$$

eine Subresultante von A_o, A_1. (Man erhält sie aus der Resultantenmatrix, indem man darin den Rand der Breite j streicht und dann die letzte Spalte durch die (i Schritte vom rechten Rand der Resultantenmatrix entfernte, verkürzte) Spalte $\begin{pmatrix} \vdots \\ a_{o,i} \\ a_{1,i} \\ \vdots \end{pmatrix}$ ersetzt.)

Im Euklidischen Algorithmus (2) für A_o, A_1 schreiben wir

$$A_\lambda = \sum_{\nu=o}^{n_\lambda} a_{\lambda,\nu} \cdot T^\nu , \quad a_{\lambda,n_\lambda} \neq 0, \text{ und } Q_\lambda = \sum_{\mu=o}^{m_\lambda} q_{\lambda,\mu} \cdot T^\mu .$$

Die Gleichung $A_{\lambda-1} = Q_{\lambda-1} \cdot A_\lambda + A_{\lambda+1}$ zeigt, dass in der Resultantenmatrix von $(A_{\lambda-1}, A_\lambda)$ die $(n_\lambda - k)$-te Zeile, $0 \leq k < n_\lambda$, Summe aus den jeweils mit $q_{\lambda,\mu}$ multiplizierten Zeilen $n_\lambda + 1 + k + \mu$ $(o \leq \mu \leq m_{\lambda-1})$ und der Zeile

$$(0,\ldots,0,\ a_{\lambda+1,n_{\lambda+1}}, \ldots, a_{\lambda+1,o},\ \underbrace{0,\ldots 0}_{k \text{ Nullen}})$$

ist. Elementare Zeilenoperationen führen also die Resultantenmatrix von $(A_{\lambda-1}, A_\lambda)$ in die folgende Matrix über:

$$(s_{\mu,\nu})_{\substack{\mu=1,\ldots,n_{\lambda-1}+n_\lambda \\ \nu=1,\ldots,n_{\lambda-1}+n_\lambda}} = \begin{pmatrix} & a_{\lambda+1,n_{\lambda+1}} \cdots & a_{\lambda+1,o} & & 0 \\ & & \ddots & & \ddots \\ 0 & & & a_{\lambda+1,n_{\lambda+1}} \cdots & a_{\lambda+1,o} \\ & & & a_{\lambda,n_\lambda} \cdots & a_{\lambda,o} \\ & & \cdot & & \cdot \\ & \cdot & & \cdot & 0 \\ a_{\lambda,n_\lambda} & \cdots & a_{\lambda,o} & & \end{pmatrix}$$

Die ausgeübten Zeilenoperationen transformieren Zeilen, die mindestens Abstand j vom oberen Rand haben, nur mit Hilfe von Zeilen, die mindestens Abstand j vom unteren Rand der Matrix haben. Daher sind die Subresultanten von $(A_{\lambda-1}, A_\lambda)$ gerade die entsprechenden Unterdeterminanten von $(s_{\mu,\nu})_{\mu,\nu}$:

$$S_{j,i}(A_{\lambda-1}, A_\lambda) = \det(s_{\mu,\nu})_{\substack{\mu = j+1,\dots,n_{\lambda-1}+n_\lambda-j \\ \nu = j+1,\dots,n_{\lambda-1}+n_\lambda-j-1,\, n_{\lambda-1}+n_\lambda-i}}$$

Umkehr der Zeilenreihenfolge und Entwicklung nach den obersten quadratischen Untermatrizen mit $(n_{\lambda-1} - n_{\lambda+1}) = m_\lambda + m_{\lambda+1}$ Zeilen liefert:

$$(5)\quad S_{j,i}(A_{\lambda-1}, A_\lambda) = (-1)^{\left\lfloor \frac{n_{\lambda-1}+n_\lambda-2j}{2} \right\rfloor} \cdot a_{\lambda,n_\lambda}^{m_\lambda+m_{\lambda+1}} \cdot S_{j,i}(A_\lambda, A_{\lambda+1})$$

$$\text{für } 0 \le i \le j \le n_{\lambda+1}$$

Ebenso liest man aus $(s_{\mu,\nu})_{\mu,\nu}$ ab:

$$(6)\quad S_{n_\lambda-1,i}(A_{\lambda-1}, A_\lambda) = \begin{cases} (-1)^{\left\lfloor \frac{m_{\lambda-1}+2}{2} \right\rfloor} \cdot a_{\lambda,n_\lambda}^{m_{\lambda-1}+1} \cdot a_{\lambda+1,i} & \text{für } 0 \le i \le n_{\lambda+1} \\ 0 & \text{für } n_{\lambda+1} < i \le n_\lambda - 1 \end{cases}$$

$$(7)\quad S_{n_\lambda,n_\lambda}(A_{\lambda-1}, A_\lambda) = (-1)^{\left\lfloor \frac{n_{\lambda-1}}{2} \right\rfloor} \cdot a_{\lambda,n_\lambda}^{m_\lambda-1} .$$

Aus (6) und (7) erhält man durch Division und $(\lambda-1)$-maliges Anwenden von (5) im Zähler und Nenner mit den eingeführten Bezeichnungen:

LEMMA 1. Zu jedem $\lambda < l$ gibt es ein $\varepsilon \in \{+1,-1\}$, das nur von λ und den Gradzahlen $n_0,\dots,n_\lambda$ abhängt, so dass für $i \le n_{\lambda+1}$

$$a_{\lambda+1,i} = \frac{\varepsilon}{a_{\lambda,n_\lambda}} \cdot \frac{S_{n_\lambda-1,i}(A_0, A_1)}{S_{n_\lambda,n_\lambda}(A_0, A_1)} \quad \text{gilt.}$$

Für $n_{\lambda+1} < i \le n_\lambda - 1$ ist $S_{n_\lambda-1,i}(A_0, A_1) = 0$.

Wendet man weiter auf a_{λ,n_λ} das Lemma an, so erhält man

SATZ 3. Seien $A_2,\dots,A_l$ die Reste im Euklidischen Algorithmus für A_o, A_1 mit $\deg A_o \geq \deg A_1$. Jeder Koeffizient von A_λ ist bis auf das Vorzeichen Produkt von λ Quotienten von Unterdeterminanten der Resultantenmatrix von A_o, A_1. Das Vorzeichen wird durch λ und die Gradzahlen der Reste bestimmt.

Wir bezeichnen mit $U_{j,k}(A_o,A_1)$ die Untermatrix der Resultantenmatrix von A_o,A_1, die durch Streichen der ersten und letzten j Zeilen, der ersten j Spalten und der letzten k Spalten entsteht. (Es ist also $S_{j,j}(A_o,A_1) = \det U_{j,j}(A_o,A_1)$.) Mit den oben bereits benutzten Bezeichnungen gilt nun

LEMMA 2. Für $\lambda \in \{2,\dots,l\}$ und $k < n_{\lambda-1}$ hat $U_{n_{\lambda-1}-1,k}(A_o,A_1)$ genau dann maximalen Rang, wenn $k < n_\lambda$ ist.

BEWEIS. Es ist nach Lemma 1 $S_{n_{\lambda-1}-1,n_\lambda}(A_o,A_1) \neq 0$, $U_{n_{\lambda-1}-1,k}(A_o,A_1)$ hat also maximalen Rang für $k \leq n_\lambda$. Andererseits existieren zum Rest A_λ Polynome B_o,B_1 mit $\deg B_i = n_i - n_{\lambda-1}$ und $A_o \cdot B_1 + A_1 \cdot B_o = A_\lambda$. Koeffizientenvergleich bei T^ν mit $\nu > n_\lambda$ ergibt ein homogenes Gleichungssystem für die Koeffizienten der B_i. Die Matrix des Gleichungssystems, $U_{n_{\lambda-1}-1,n_\lambda+1}(A_o,A_1)$, hat also nicht maximalen Rang, und daher ebenso $U_{n_{\lambda-1}-1,k}(A_o,A_1)$ für jedes k mit $n_\lambda < k < n_{\lambda-1}$.

Nun sei weiterhin $n_o \geq n_1$. Für jedes Polynom $P = \sum_{\nu=0}^{n} p_\nu \cdot T^\nu \in K[T]$ schreiben wir $\underline{P} := (P_n,\dots,P_o) \in K^{n+1}$.

$D_{m_o,\dots,m_{l-1},m_l}$ bezeichne die lokal abgeschlossene Menge aller Paare $(\underline{A}_o,\underline{A}_1) \in K^{n_o+n_1+2}$, deren zugehörigen Polynompaare (A_o,A_1) eine Euklidische Entwicklung $(Q_o,\dots,Q_{l-1},A_l)$ mit den Gradzahlen $m_o,\dots,m_{l-1},m_l$ haben.

D_o bestehe aus den Paaren $(\underline{A}_o,\underline{A}_1) \in K^{n_o+n_1+2}$ mit $\deg A_o < n_o$ oder $\deg A_1 < n_1$.

SATZ 4. Sei $n_1 = m_1+\dots+m_l$, $n_o = n_1+m_o$. Für den Grad d von $D_{m_o,\dots,m_l}$ in $K^{n_o+n_1+2}$ gilt:

$$\frac{n_o!}{m_o!\cdot\ldots\cdot m_l!\cdot(m_o+1)\cdot(m_o+m_1+1)\cdot\ldots\cdot(m_o+\dots+m_{l-1}+1)} \leq d .$$

BEWEIS. Sei $n_\lambda = m_\lambda + m_{\lambda+1}+\dots+m_l$ für jedes λ.
lc P bezeichnet den Leitkoeffizienten des Polynoms P.
Der Morphismus

$$\varphi:\left\{(v,\underline{Q}_o,\dots,\underline{Q}_{l-1},\underline{A}_l) \in K \times K^{n_o+l+1} : \deg A_l=n_l, \forall\lambda \ \deg Q_\lambda=m_\lambda,\ \mathrm{lc}\,Q_\lambda=1\right\} \longrightarrow K^{n_o+2}$$

$$(v,Q_o,\dots,Q_{l-1},\underline{A}_l) \mapsto (v,\underline{B})$$

mit $$(1,0)\cdot\begin{pmatrix}Q_o & v\\ v & 0\end{pmatrix}\cdot\begin{pmatrix}Q_1 & v\\ v & 0\end{pmatrix}\cdot\ \ldots\ \cdot\begin{pmatrix}Q_{l-1} & v\\ v & 0\end{pmatrix}\cdot\begin{pmatrix}A_l\\ 0\end{pmatrix} = (B)$$

ist dominant, denn jede Komponente von

$$\varphi^{-1}(0,\underline{B}) = \left\{(0,\underline{Q}_o,\dots,\underline{A}_l) : Q_o\cdot Q_1\cdot\ldots\cdot Q_{l-1}\cdot A_l = B,\ \forall\lambda \quad \mathrm{lc}\,Q_\lambda = 1\right\}$$

ist nulldimensional. Speziell für ein B mit paarweise verschiedenen Nullstellen ist $\#\varphi^{-1}(0,B) = \dfrac{n_o!}{m_o!\cdot\ldots\cdot m_l!}$.
Es gibt also auch ein $v \neq o$ und ein A mit $\deg A = n_o$ und endlichem $\#\varphi^{-1}(v,\underline{A}) \geq \dfrac{n_o!}{m_o!\cdot\ldots\cdot m_l!}$ (Vergleiche z.B. Prop.1 aus [5] von Heintz). Wegen

$$\begin{pmatrix}Q_o & v\\ v & 0\end{pmatrix}\cdot\ \ldots\ \cdot\begin{pmatrix}Q_{l-1} & v\\ v & 0\end{pmatrix}\cdot\begin{pmatrix}A_l\\ 0\end{pmatrix} = \begin{pmatrix}Q_o/v & 1\\ 1 & 0\end{pmatrix}\cdot\ \ldots\ \cdot\begin{pmatrix}Q_{l-1}/v & 1\\ 1 & 0\end{pmatrix}\cdot\begin{pmatrix}v^l\cdot A_l\\ 0\end{pmatrix}$$

haben wir eine Bijektion zwischen $\varphi^{-1}(v,\underline{A})$ und

$$S = \left\{ (\underline{A}_o,\underline{A}_1) \in K^{n_o+n_1+2} : \exists\, Q_o,\dots,Q_{l-1},A_l \;\forall \lambda \; \deg Q_\lambda = m_\lambda,\; lc\, Q_\lambda = \frac{1}{v}, \right.$$

$$\left. \begin{pmatrix} Q_o & 1 \\ 1 & 0 \end{pmatrix} \cdot \;\dots\; \cdot \begin{pmatrix} Q_{l-1} & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} A_l \\ 0 \end{pmatrix} = \begin{pmatrix} A_o \\ A_1 \end{pmatrix}, A_o = A \right\}$$

$$= \left\{ (\underline{A}_o,\underline{A}_1) \in D_{m_o,\dots,m_l} : \forall \lambda \geq 2 \;\; lc\, A_\lambda = v^\lambda \cdot lc\, A, \;\; A_o = A \right\},$$

wo $A_2,\dots,A_l$ die Reste im Euklidischen Algorithmus von A_o,A_1 $((\underline{A}_o,\underline{A}_1) \in D_{m_o,\dots,m_l})$ bezeichnen (s. Gleichung (2) und (3)). Mit Lemma 1 erhalten wir weiter

$$S = \left\{ (\underline{A}_o,\underline{A}_1) \in D_{m_o,\dots,m_l} : \;\; A_o = A \,, \;\; lc\, A_1 = v \cdot lc\, A, \right.$$

$$\left. \forall \lambda \geq 1 \;\; v^{2\lambda+1} \cdot (lcA)^2 \cdot S_{n_\lambda,n_\lambda}(A,A_1) = \varepsilon_\lambda S_{n_\lambda-1,n_{\lambda+1}}(A,A_1) \right\},$$

wo die ε_λ für wohlbestimmte Vorzeichen stehen.

$S_{n_\lambda,n_\lambda}(A,A_1)$ und $S_{n_\lambda-1,n_{\lambda+1}}(A,A_1)$ haben in den Koeffizienten von A_1 die Grade n_o-n_λ und $n_o-n_\lambda+1 = m_o+m_1+\dots+m_{\lambda-1} + 1$.

Damit folgt die Behauptung.

Mit diesem Satz zeigen wir das Hauptresultat dieses Paragraphen: Die Aufgabe, aus den Koeffizienten von A_o, A_1 die Gradzahlen $m_o,\dots,m_l$ der Euklidischen Entwicklung von A_o,A_1 zu berechnen, hat "im schwierigsten Fall" die multiplikative Komplexität

$$\asymp \;\; n_o \cdot \lg n_o \; .$$

Die obere Schranke liefert der Algorithmus aus [8].

Die Abschätzung nach unten formulieren wir präzis im folgenden

KOROLLAR. <u>(Berechnung der Gradzahlen der Euklidischen Entwicklung)</u>. <u>Es sei</u> $n_o = \sum_{\lambda=o}^{l} m_\lambda$ <u>mit</u> $o < m_\lambda$ für $o < \lambda < l$ <u>und es sei</u>

$$c \cdot n_o \leq \# \left\{ \lambda : 1 < m_\lambda \right\}.$$

Ist die Indikatorfunktion von $D_{m_0,\dots,m_1}$ in der Zeit t berechenbar, so gilt für fast alle $(\underline{A}_0,\underline{A}_1) \in D_{m_0,\dots,m_1}$

$$c \cdot n_0 \lg n_0 - 3 \cdot n_0 \leq t(\underline{A}_0,\underline{A}_1) .$$

BEWEIS. Ist π eine endliche Partition von $K^{n_0+n_1+2}$ $(n_1 = n_0 - m_0)$ in lokal abgeschlossene Stücke, so wird $D_{\underline{m}}$ von einem $D \in \pi$ in einer dichten Menge geschnitten, denn $D_{\underline{m}}$ ist als Bild der Menge aller Euklidischen Entwicklungen mit den Gradzahlen $m_0,\dots,m_1$ irreduzibel. Nun gilt für die Grade in $K^{n_0+n_1+2}$ beziehungsweise $K^{n_0+n_1+2}$

$$\deg(\text{graph } f\restriction_D) \geq \deg(D \cap D_{\underline{m}}) = \deg D_{\underline{m}}.$$

Mit Satz 4 und dem zitierten Satz aus [13] von Strassen folgt für alle $(\underline{A}_0,\underline{A}_1)$ aus der in $D_{\underline{m}}$ dichten Menge $D \cap D_{\underline{m}}$

$$\lg \frac{n_0!}{m_0! \dots m_1!(m_0+1) \dots (m_0+\dots+m_1+1)} \leq t(\underline{A}_0,\underline{A}_1).$$

Die linke Seite der Ungleichung ist nie kleiner als

$$\sum_{1<m_\lambda} m_\lambda \cdot \lg \frac{n_0}{m_\lambda} + (l+1-k)\cdot \lg n_0 - 2n_0 - l \cdot \lg n_0$$

mit $k := \# \{ \lambda : 1 < m_\lambda \}$, denn es ist ja $n \cdot \lg n - 2 \cdot n \leq \lg(n!)$.

Für $3 \leq n_0$ zeigen wir

$$\text{(i)} \qquad 2 \cdot k \cdot \lg n_0 - n_0 \leq \sum_{1<m_\lambda} m_\lambda \cdot \lg \frac{n_0}{m_\lambda} ,$$

woraus sich dann die Behauptung ergibt, die ja für $n_0 < 3$ trivial ist.

$\binom{m}{2}^{\frac{2}{m-2}}$ ist antiton in $m > 2$, also ist für $4 \leq m$

$$\binom{m}{2}^{\frac{2}{m-2}} \leq 2 .$$

$m \leq n \in \mathbb{N}$ und $4 \leq m$ hat also $m \cdot \left(\frac{m}{2}\right)^{\frac{2}{m-2}} \leq 2 \cdot n$

zur Folge. Diese Ungleichung prüft man leicht auch für $m = 3$ nach. Logarithmieren ergibt

$(m-2) \cdot \lg m + 2 \cdot \lg m - 2 \leq (m-2) \cdot \lg n + m - 2$

und damit

$$2 \cdot \lg n - m \leq m \cdot \lg \frac{n}{m} .$$

Dies ist sogar für alle $m,n \in \mathbb{N}$ mit $1 < m \leq n$ richtig. k mal, nämlich wenn $1 < m_\lambda$ ist, schätzen wir so $m_\lambda \cdot \lg \frac{n_o}{m_\lambda}$ durch $2 \cdot \lg n_o - m_\lambda$ nach unten ab und erhalten (i).

BEMERKUNGEN.

1. Für $\#\left\{\lambda : 1 < m_\lambda\right\} \leq C$ liefert der Grad nur triviale Schranken:

$$\deg D_{\underline{m}} \leq 2^{C \cdot (n_o + n_1)}$$

2. Auch der Grad des Komplementes $C_{\underline{m}}$ von $D_{\underline{m}}$ in $K^{n_o+n_1+2}$ liefert nur triviale Schranken: Entweder ist $C_{\underline{m}}$ dicht in $K^{n_o+n_1+2}$ oder es ist – im "Normalfall" $m_1 = m_2 = \ldots = m_{l-1}, m_l = 0$ –

$$\deg C_{\underline{m}} \leq n_1 \cdot 2^{n_o+n_1}$$

BEWEIS. 1. Aus Lemma 1 und Lemma 2 ergibt sich

$$D_{\underline{m}} = \Big\{ (\underline{A}_o, \underline{A}_1) : \forall \lambda \in \{2,\ldots,l\} \ S_{n_{\lambda-1}-1,n_\lambda}(A_o,A_1) \neq 0,$$
$$1 < m_\lambda \Rightarrow \det\left(U_{n_{\lambda-1}-1,n_\lambda+1}(A_o,A_1) \cdot \left(U_{n_{\lambda-1}-1,n_\lambda+1}(A_o,A_1)\right)^T \right) = 0 \Big\}.$$

2. Für $\lambda \in \{1,\ldots,n_1-1\}$ sei

$$V_\lambda := \Big\{ (\underline{A}_o, \underline{A}_1) : \exists\ Q_o, Q_1, \ldots, Q_\lambda,\ A_{\lambda+1}, A_{\lambda+2}\ \deg Q_1 = \ldots = \deg Q_\lambda = 1,$$
$$\deg A_{\lambda+2} \leq (\deg A_{\lambda+1}) - 2,\ \deg A_o = n_o,\ \deg A_1 = n_1,$$
$$\begin{pmatrix} A_o \\ A_1 \end{pmatrix} = \begin{pmatrix} Q_o & 1 \\ 1 & 0 \end{pmatrix} \cdot \ldots \cdot \begin{pmatrix} Q & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} A_{\lambda+1} \\ A_{\lambda+2} \end{pmatrix} \Big\} .$$

Dann gilt $C_{\underline{m}} = D_o \cup \bigcup_{\lambda=1}^{n_1-1} V_\lambda$ und wieder wegen Lemma 1 und Lemma 2 $\deg V_\lambda \leq 2^{n_o+n_1}$ und damit die Behauptung.

§ 4. DAS RECHNEN MIT KETTENBRÜCHEN.

Lässt man in der Euklidischen Entwicklung $(Q_o,\dots,Q_{l-1},A_l)$ von (A_o,A_1) den g.g.T. A_l fort, so bleibt ein nur noch von der rationalen Funktion $\frac{A_o}{A_1} \in K(T)$ abhängendes Polynom-Tupel $(Q_o,\dots,Q_{l-1})$ bestehen, die sogenannte Kettenbruchdarstellung von $\frac{A_o}{A_1}$. Jedes Element $A \in K(T)$ hat genau eine Darstellung als Kettenbruch $(Q_o,\dots,Q_{l-1}) \in K[T]^l$ mit $o < l$ und $1 \leq \deg Q_\lambda$ für $1 \leq \lambda$. Umgekehrt stellt jeder solche Kettenbruch genau ein $A \in K(T)$ dar, nämlich

(8) $$A = \frac{[Q_o,\dots,Q_{l-1}]}{[Q_1,\dots,Q_{l-1}]} .$$

Wir behandeln nun das Rechnen mit diesen Kettenbrüchen. Aus den n Koeffizienten der Kettenbruchdarstellung von $A \in K(T)^x$ lassen sich mit $O(n)$ nichtskalaren Multiplikationen und Divisionen die Koeffizienten der Kettenbruchdarstellung von A^{-1} berechnen. Auch die Multiplikationen eines Kettenbruchs mit einem Element aus K ist in linearer Zeit ausführbar. Anders die Addition, die Multiplikation und das Auswerten an $\sum_{\lambda=o}^{l-1} \deg Q_\lambda$ Stellen. Zumindest im Sinne einer "Untersuchung des schwierigsten Falles" haben diese Aufgaben sämtlich eine multiplikative Komplexität

$$\asymp n \cdot \lg n,$$

wo n die Anzahl der Inputvariablen ist.

INVERSION. _Stellt_ $(Q_o,\dots,Q_{l-1})$ _die rationale Funktion_ $A \in K(T)$ _dar und ist_ $1 \leq \deg Q_o$, _so ist_ $(0,Q_o,\dots,Q_{l-1})$

die Kettenbruchdarstellung von A^{-1}. Im Falle $Q_o = 0$ ist es natürlich $(Q_1, Q_2, \ldots, Q_{l-1})$ und im Falle $\deg Q_o = 0$ ist es $(Q_o^{-1}, -Q_o - Q_o^2 Q_1, -Q_o^{-2} Q_2, -Q_o^2 Q_3, -Q_o^{-2} Q_4, \ldots)$ mit $-Q_o^{-2} \cdot Q_{l-1}$ oder $-Q_o^2 \cdot Q_{l-1}$ endend, je nach der Parität von l.

BEWEIS. Wir zeigen für $\deg Q_o = o$ und gerades l

$$\frac{[Q_o^{-1}, -Q_o - Q_o^2 Q_1, -Q_o^{-2} Q_2, \ldots, -Q_o^2 Q_{l-1}]}{[-Q_o - Q_o^2 Q_1, -Q_o^{-2} Q_2, \ldots, -Q_o^2 Q_{l-1}]} = \frac{[Q_1, \ldots, Q_{l-1}]}{[Q_o, \ldots, Q_{l-1}]} .$$

Die Beweise der anderen Aussagen, auch die der folgenden über skalare Vielfache, verlaufen ähnlich. Aus der Definition des Eulerschen Symbols ergibt sich $[Q_o^{-1}, -Q_o - Q_o^2 Q_1, -Q_o^{-2} Q_2, \ldots, -Q_o^2 Q_{l-1}] =$

$$[Q_o^{-1}, -Q_o - Q_o^2 Q_1] \cdot [-Q_o^{-2} Q_2, \ldots, -Q_o^2 Q_{l-1}] + Q_o^{-1} \cdot [-Q_o^2 Q_3, \ldots, -Q_o^2 Q_{l-1}]$$

$$= (-Q_o Q_1) \cdot [Q_2, \ldots, Q_{l-1}] + Q_o^{-1} \cdot (-Q_o^2) \cdot [Q_3, \ldots, Q_{l-1}]$$

$$= -Q_o \cdot [Q_1, \ldots, Q_{l-1}]$$ und

$$[-Q_o - Q_o^2 Q_1, -Q_o^{-2} Q_2, \ldots, -Q_o^2 Q_{l-1}]$$

$$= (-Q_o - Q_o^2 Q_1) \cdot [Q_2, \ldots, Q_{l-1}] + (-Q_o^2) \cdot [Q_3, \ldots, Q_{l-1}]$$

$$= (-Q_o) \cdot \Big([Q_o, Q_1] \cdot [Q_2, \ldots, Q_{l-1}] + Q_o \cdot [Q_3, \ldots, Q_{l-1}] \Big)$$

$$= -Q_o \cdot [Q_o, \ldots, Q_{l-1}]$$ und damit die Behauptung.

SKALARE VIELFACHE. Ist $(Q_o, \ldots, Q_{l-1})$ die Kettenbruchdarstellung von A und $b \in K^{\times}$, so wird $b \cdot A$ von dem Kettenbruch $(b \cdot Q_o, b^{-1} \cdot Q_1, b \cdot Q_2, b^{-1} \cdot Q_3, \ldots)$ dargestellt, wieder je nach der Parität von l endend.

MULTIPLIKATION. Die Berechnung der Koeffizienten der Q_λ aus den Koeffizienten von A_o und A_1 wird in [13] untersucht. Mit den dort bewiesenen Sätzen zeigt sich: Für fast alle $\frac{A_o}{A_1} \in K(T)$ mit $\deg A_o + \deg A_1 \leq n$ ist

$\frac{n}{2} \cdot \lg \frac{n}{4}$ eine untere Schranke für die Berechnungszeit nach unserer Zählung. Berechnet man aus den Kettenbrüchen $(Q_o,\ldots,Q_{l-1})$, $(P_o,\ldots,P_{g-1})$ die Kettenbruchdarstellung $(R_o,\ldots,R_{s-1})$ des Produktes der zugehörigen rationalen Funktionen, so löst man (speziell im Fall $l = 1$, $P_o = 0$ und $g = 2$) die Aufgabe, aus Q_o und P_1 die Kettenbruchdarstellung $(R_o,\ldots,R_{s-1})$ von $\frac{Q_o}{P_1}$ zu berechnen. Sind die Q_λ und P_γ durch insgesamt $n+2$ Koeffizienten gegeben, so braucht man daher zur Berechnung der Koeffizienten von $(R_o,\ldots,R_{s-1})$ im allgemeinen mindestens $\frac{n}{2} \cdot \lg \frac{n}{4}$ Multiplikationen. Durch Umrechnung über die zugehörigen rationalen Funktionen lässt sich andererseits die Berechnung mit $90 \cdot n \cdot \lg n + 470 \cdot n$ Multiplikationen ausführen.

ADDITION. Für beliebige $Q_\lambda \in K[T]$ und $l \geq 2$ gilt

$$[-Q_o,-Q_1,\ldots,-Q_{l-2}]\cdot[Q_1,\ldots,Q_{l-1}] + [-Q_1,\ldots,-Q_{l-2}]\cdot[Q_o,\ldots,Q_{l-1}] = 1$$

(Zum Induktionsbeweis schreibt man im Schritt die linke Seite so:

$$[-Q_o,\ldots,-Q_{l-2}]\cdot[Q_1,\ldots,Q_{l-2}]\cdot Q_{l-1} + [-Q_o,\ldots,-Q_{l-2}]\cdot[Q_1,\ldots,Q_{l-3}] +$$
$$[-Q_1,\ldots,-Q_{l-2}]\cdot[Q_o,\ldots,Q_{l-2}]\cdot Q_{l-1} + [-Q_1,\ldots,-Q_{l-2}]\cdot[Q_o,\ldots,Q_{l-3}]$$

und beachtet, dass sich der erste mit dem dritten Summanden weghebt.)

Es ist also

$$\frac{[Q_o,\ldots,Q_{l-1}]}{[Q_1,\ldots,Q_{l-1}]} + \frac{[-Q_o,\ldots,-Q_{l-2}]}{[-Q_1,\ldots,-Q_{l-2}]} = \frac{1}{R}$$

mit $R = [Q_1,\ldots,Q_{l-1}]\cdot[-Q_1,\ldots,-Q_{l-2}]$. Die Summe der von $(Q_o,\ldots,Q_{l-1})$ und $(-Q_o,\ldots,-Q_{l-2})$ dargestellten rationalen Funktion hat die Kettenbruchdarstellung $(0,R)$.

Seien nun $\hat{Q}_1,\ldots,\hat{Q}_{l-1}$ lineare Polynome ("Normalfall") jeweils mit Unbestimmten als Koeffizienten. Nun ist

$\hat{R} = [\hat{Q}_1,\dots,\hat{Q}_{l-1}]\cdot[-\hat{Q}_1,\dots,-\hat{Q}_{l-2}] \in K(\underline{\hat{Q}}_1,\dots,\underline{\hat{Q}}_{l-1})[T]$

($\underline{P}$ steht für den Koeffizientenvektor des Polynoms P).

L sei die (nichtskalare) multiplikative Komplexität in $K(\underline{\hat{Q}}_1,\dots,\underline{\hat{Q}}_{l-1})$ als K-Algebra über K und den Unbestimmten.

Nun ist

(9) $$n\cdot \lg \frac{n}{e} \leq L(\underline{\hat{R}})$$

mit $n = l-1$. Umgekehrt lässt sich aus den Koeffizienten zweier Kettenbrüche $(Q_o,\dots,Q_{l-1})$, $(P_o,\dots,P_{g-1})$ die des Summenkettenbruches in der Zeit

$$180\cdot n\cdot \lg n + 940\cdot n$$

durch Umrechnung über die zugehörigen rationalen Funktionen berechnen

$$(n := \max\left\{\sum_{\lambda=o}^{l-1} \deg Q_\lambda \;,\; \sum_{\gamma=o}^{g-1} \deg P_\gamma\right\}) .$$

Zum Beweis von (9) benötigen wir das folgende

LEMMA (V.Strassen [13]). Seien $y,x_1,\dots,x_n$ Unbestimmte über dem algebraisch abgeschlossenen Körper K und seien $f_1,\dots,f_r \in K[y,x_1,\dots,x_n]$. Für $v \in K$ sei $F_v \subset K^{n+r}$ der Graph der Abbildung $(u_1,\dots,u_n) \mapsto (f_1(v,\underline{u}),\dots,f_r(v,\underline{u}))$. Dann definiert $v \mapsto \deg F_v$ eine unterhalbstetige Abbildung von K nach $\mathbb{N}$.

BEWEIS von (9). Wir wenden das Lemma auf den Graphen F_v von

$$(\underline{Q}_1,\dots,\underline{Q}_{l-1}) \mapsto \underline{R}$$

mit $$R = \begin{cases} v^{2l-3}\cdot\left[\frac{Q_1}{v},\dots,\frac{Q_{l-1}}{v}\right]\cdot\left[-\frac{Q_1}{v},\dots,-\frac{Q_{l-2}}{v}\right] & \text{für } v \in K^{\times} \\ (-1)^{l-2}\cdot Q_1^2\cdot Q_2^2\cdot\ldots\cdot Q_{l-2}^2\cdot Q_{l-1} & \text{für } v = o \end{cases}$$

an. Nun ist für paarweise verschiedene $u_1,\dots,u_{l-1} \in K$

$$\# \; F_o \cap \left\{(\underline{Q}_1,\dots,\underline{Q}_{l-1},\underline{R}) : \forall \lambda \;\; \mathrm{lc}\, Q_\lambda = 1,\; R(u_1)=\ldots=R(u_{l-1})=0\right\} = n!.$$

Andererseits ist für jedes $v \in K^{\times}$

$$\deg F_v = \deg F_1 \leq 2^{L(\underline{\hat{R}})} .$$

AUSWERTEN EINES KETTENBRUCHS AN VIELEN STELLEN.

$x_1,\dots,x_m$ seien Unbestimmte über K, $\hat{Q}_0,\dots,\hat{Q}_{l-1}$ seien Polynome in T mit weiteren Unbestimmten als Koeffizienten ($\deg \hat{Q}_\lambda = m_\lambda$, $n_0 := \sum_{\lambda=0}^{l-1} m_\lambda$). L bezeichne die multiplikative Komplexität in $K(\underline{x}_1\ \hat{\underline{Q}}_0,\dots,\hat{\underline{Q}}_{l-1})$ (Bezeichnungen wie oben). Sei A die durch $(\hat{Q}_0,\dots,\hat{Q}_{l-1})$ dargestellte rationale Funktion. Dann gilt

(10) $\qquad m\cdot \lg n_0 \leq L(A(x_1),\dots,A(x_m))$

Für $m \geq n_0$ stimmt diese untere Schranke bis auf einen konstanten Faktor mit der oberen Schranke überein, die sich aus [13] und [4] ergibt.

BEWEIS VON (10). Der Morphismus

$$(v,\underline{P}_0,\dots,\underline{P}_{l-1}) \mapsto (v,\underline{B}_0)$$

von $K \times K^{m_0+1} \times \dots \times K^{m_{l-1}+1}$ nach $K \times K^{n_0+1}$

mit $(B_0) = (1,0)\cdot\begin{pmatrix}P_0 & v\\ v & 0\end{pmatrix}\cdot \;\dots\; \cdot\begin{pmatrix}P_{l-1} & v\\ v & 0\end{pmatrix}\cdot\begin{pmatrix}1\\ 0\end{pmatrix}$

ist dominant, denn das Urbild von $(o,\underline{B}_0)$ mit $\underline{B}_0 \neq 0$ ist stets $(l-1)$-dimensional. Wir können daher $P_0,\dots,P_{l-1}$ und $v \neq o$ so wählen, dass das zugeordnete B_0 n_0 verschiedene Nullstellen hat. Für so gewählte P_λ, v und B_0 ist

$$(B_1) := (0,1)\cdot\begin{pmatrix}P_0 & v\\ v & 0\end{pmatrix}\cdot \dots \begin{pmatrix}P_{l-1} & v\\ v & 0\end{pmatrix}\cdot\begin{pmatrix}1\\ 0\end{pmatrix}$$

teilerfremd zu B_0. Die in K offene Menge

$\{z \in K : B_0 - z\cdot B_1$ hat n_0 verschiedene Nullstellen$\}$

ist nicht leer, enthält also paarweise verschiedene $z_1,\dots,z_m$. Nun können wir unter Benützung von (3) und (4) aus § 3 den Grad von

$$F := \Big\{ (u_1,\dots,u_m,\underline{Q}_o,\dots,\underline{Q}_{l-1},v_1,\dots,v_m) : \ \forall \lambda \quad \deg Q_\lambda = m_\lambda ,$$

$$\forall \mu \le m \quad \big[Q_o,\dots,Q_{l-1}\big](u_\mu) = v_\mu \cdot \big[Q_1,\dots,Q_{l-1}\big](u_\mu)$$

$$\big[Q_1,\dots,Q_{l-1}\big](u_\mu) \neq 0 \quad \Big\}$$

abschätzen:

$$\# \ F \cap \Big\{ (u,\underline{Q}_o,\dots,\underline{Q}_{l-1},v) : \forall \lambda \quad Q_\lambda = v^{-1} P_\lambda \ , \ \forall \mu \quad v_\mu = z_\mu \Big\}$$

$$= \# \Big\{ \underline{u} : \ \forall \mu \ \ B_o(u_\mu) - z_\mu \cdot B_1(u_\mu) = 0 \Big\} = m^n.$$

($B_o(u) - z_\mu \cdot B_1(u) = 0$ impliziert $B_1(u) \neq 0$, da

B_o, B_1 teilerfremd in $K[\,T\,]$ sind.)

LITERATUR

[1] M.Bôcher : Introduction to higher algebra, 1967.

[2] A.Borodin, R.Moenck: Fast Modular Transforms, J. of Comp. and Syst. Sc., 1974.

[3] G.E.Collins: The calculation of multivariate polynomial resultants; J.A.C.M., 1971.

[4] C.M.Fiduccia: Polynomial evaluation via the division algorithm; Proc. 4 th Ann.ACM Symp. on Theory of Comp., 1972.

[5] J.Heintz: Dissertation; in Vorbereitung, 1978.

[6] E.Horowitz: A fast method for interpolation, using preconditioning; Inf. Process. Letters, 1972.

[7] R.Moenck: Studies in fast algebraic algorithms; Univ. of Toronto Comp. Science Tech. Report, 1973.

[8] A.Schönhage: Schnelle Berechnung von Kettenbruchentwicklungen; Acta Informatica, 1971.

[9] M.Sieveking: An algorithm for division of power series; Computing, 1972.

[10] V.Strassen: Die Berechnungskomplexität der elementar-symmetrischen Funktionen und Interpolations-koeffizienten; Num. Math. 1973.

[11] " : Vermeidung von Divisionen; J. Reine Angew. Math., 1973.

[12] " : Some results in algebraic complexity theory; Proceedings Int. Congr. Math. Vancouver, 1974.

[13] " : The computational complexity of continued fractions; in Vorbereitung, 1974.

[14] " : Die Berechnungskomplexität der symbolischen Differentiation von Interpolationspolynomen; Theor. Comp. Sci, 1975.

CURRICULUM VITAE

Am 29. April 1948 wurde ich, Peter Schuster, in Reinbek in Deutschland geboren. Ich bin deutscher Staatsangehöriger. Nach dem Besuch der Primarschule besuchte ich von 1958 bis 1961 das Arndt-Gymnasium in Bonn (Deutschland) und von 1961 bis 1967 die Deutsche Schule in Paris (Frankreich), wo ich das deutsche Reifezeugnis erhielt. Dann studierte ich an der Universität Zürich Mathematik mit den Nebenfächern Wirtschaftswissenschaft und Physik. Dort und an der Eidgenössischen Technischen Hochschule besuchte ich Vorlesungen und Seminare u.a. bei den Professoren Eckmann, Engeler, Gabriel, Gross, Hill, P.Huber, Jarchow, Karrer, Keller, Matzinger, Specker, Stoss, Strassen, Strebel, van der Waerden. 1974 legte ich meine Diplomprüfung in Mathematik und den genannten Nebenfächern ab.

Die vorliegende Arbeit entstand unter der Leitung von Herrn Prof. V. Strassen.

Seit 1978 bin ich als wissenschaftlicher Angestellter am Mathematischen Institut der Universität Tübingen tätig. Hiervor arbeitete ich nacheinander als Assistent am Mathematischen Institut und Seminar für Angewandte Mathematik der Universität Zürich.